

WHAT IS CLAIMED IS:

1 1. A device for processing an image, the device comprising:
2 a decryption module configured to receive graphics data, wherein at least a
3 portion of the received graphics data is encrypted, and to decrypt the graphics data based at
4 least in part on a decryption parameter;
5 a key module configured to receive key data and to provide the decryption
6 parameter to the decryption module in response to the key data; and
7 an image generation module coupled to receive the decrypted graphics data
8 from the decryption module and configured to transform the decrypted graphics data to
9 displayable image data.

1 2. The device of claim 1 wherein the decryption module is further
2 configured to provide the encrypted graphics data to the image generation module in the
3 event that the key module does not provide the decryption parameter.

1 3. The device of claim 1 wherein the encrypted portion of the graphics
2 data is encrypted by applying a perturbation, the perturbation being removable by the
3 decryption module.

1 4. The device of claim 1 wherein the key data includes the decryption
2 parameter.

1 5. The device of claim 1 wherein the key module is further configured to
2 compute the decryption parameter using the key data.

1 6. The device of claim 1 wherein the key module includes a receptacle for
2 a key device and wherein the key module is further configured to obtain the key data from the
3 key device.

1 7. The device of claim 6 wherein the decryption parameter corresponds to
2 the presence or absence of the key device in the receptacle.

1 8. The device of claim 6 wherein the key device is configured to store the
2 key data and the key module is configured to read the key data when the key device is present
3 in the receptacle.

1 9. The device of claim 1 wherein the key module receives the key data
2 from a sender and the decryption module receives the graphics data from the same sender.

1 10. The device of claim 1 wherein the key module is further configured to
2 receive either of first key data and second key data and to provide a first decryption
3 parameter in response to the first key data and a second decryption parameter in response to
4 the second key data,
5 wherein in response to the first decryption parameter, the decryption module
6 completely decrypts the graphics data and, in response to the second decryption parameter,
7 the decryption module decrypts the graphics data with a residual distortion.

1 11. A system for generating images, the system comprising:
2 a sender device configured to send graphics data via a communication
3 channel, wherein at least a portion of the graphics data is encrypted;
4 a recipient device including:
5 a decryption module configured to receive the encrypted graphics data
6 and to decrypt the graphics data based at least in part on a decryption parameter;
7 a key module configured to receive key data and to provide the
8 decryption parameter to the decryption module in response to the key data; and
9 an image generation module coupled to receive the decrypted graphics
10 data from the decryption module and configured to transform the graphics data to displayable
11 image data.

1 12. The system of claim 11 wherein the sender device and the recipient
2 device communicate via a bus.

1 13. The system of claim 12 wherein the sender device is a central
2 processing unit and the recipient device includes a graphics processing unit.

1 14. The system of claim 11 wherein the sender device and the recipient
2 device communicate via a network.

1 15. The system of claim 11 wherein the key module includes a receptacle
2 for a key device, the key device providing the key data to the key module.

1 16. The system of claim 11 wherein the key data includes the decryption
2 parameter.

1 17. The system of claim 11 wherein the key module is further configured
2 to compute the decryption parameter using the received key data.

1 18. The system of claim 11 wherein the key module is configured to
2 receive either of first key data and second key data and further configured to provide a first
3 decryption parameter in response to the first key data and a second decryption parameter in
4 response to the second key data,
5 wherein in response to the first decryption parameter, the decryption module
6 completely decrypts the graphics data and, in response to the second decryption parameter,
7 the decryption module decrypts the graphics data with a residual distortion.

1 19. A method of generating an image, the method comprising:
2 receiving graphics data for the image, wherein at least a portion of the
3 received graphics data is encrypted;
4 determining whether a key is present; and
5 in response to determining that the key is present:
6 decrypting the encrypted portion of the graphics data; and
7 rendering an image using the decrypted graphics data.

1 20. The method of claim 19, further comprising:
2 in response to determining that the key is not present, rendering an image
3 using the received graphics data including the encrypted portion.

1 21. The method of claim 19 further comprising:
2 in response to determining that the key is present, extracting a decryption
3 parameter from the key,
4 wherein the act of decrypting the encrypted portion of the graphics data is
5 responsive to the decryption parameter.

1 22. The method of claim 19, further comprising, prior to the act of
2 receiving the graphics data:
3 encrypting at least a portion of the graphics data; and

4 transmitting the graphics data.

1 23. The method of claim 22 wherein the act of transmitting the graphics
2 data is performed using a system bus.

1 24. The method of claim 23 wherein the act of encrypting is performed by
2 a central processing unit executing a graphics driver program.

1 25. The method of claim 22 wherein the act of transmitting the graphics
2 data is performed using a network.

1 26. The method of claim 19 wherein the act of determining whether the
2 key is present includes detecting a presence or absence of a key device.

1 27. The method of claim 19 wherein the act of determining whether the
2 key is present includes detecting a presence or absence of key data.

1 28. The method of claim 19 wherein the act of decrypting the graphics data
2 includes:
3 restoring the graphics data to its unencrypted state; and
4 perturbing a parameter value of the restored graphics data based on a
5 perturbation parameter.

1 29. The method of claim 28 wherein the parameter value is a vertex
2 coordinate of a primitive.

1 30. The method of claim 28 wherein the perturbation parameter is
2 determined from the key.

1 31. The method of claim 30 wherein the perturbation parameter
2 corresponds to a clearance level associated with the key.

1 32. A method for sharing encrypted graphics data among a plurality of
2 users, the method comprising:
3 associating each of the plurality of users with a respective one of a plurality of
4 keys for decrypting the encrypted graphics data;
5 receiving the encrypted graphics data at a recipient device;

6 receiving one of the plurality of keys at the recipient device, wherein the one
7 of the plurality of keys is provided by the associated user; and
8 decrypting the encrypted graphics data based at least in part on the received
9 key.

1 33. The method of claim 32 wherein each key includes an identifier of a
2 clearance level and the act of decrypting the graphics data depends at least in part on the
3 clearance level.

1 34. The method of claim 33 wherein during the act of decrypting, a
2 perturbation is applied to the graphics data, the size of the perturbation being dependent on
3 the clearance level.

1 35. The method of claim 33 wherein during the act of decrypting, the
2 clearance level is used to determine whether to discard a portion of the graphics data.

1 36. The method of claim 32 wherein the act of associating each of the
2 plurality of users with a respective one of the plurality of keys includes providing a respective
3 hardware device for each user, each hardware device storing key data, and wherein the act of
4 receiving one of the plurality of keys includes communicating with the hardware device.

1 37. The method of claim 36 wherein communicating with the hardware
2 device includes receiving the hardware device in a receptacle of the recipient device.

1 38. The method of claim 32 wherein the act of associating each of the
2 plurality of users with a respective one of the plurality of keys includes providing a password
3 for each user, and wherein the act of receiving one of the plurality of keys includes receiving
4 the password.